Doc code: IDS Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-09)
Approved for use through 03/31/2009. OMB 0651-0031
Ormation Disclosure Statement (IDS) Filed
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| INFORMATION DISCLOSURE<br>STATEMENT BY APPLICANT<br>(Not for submission under 37 CFR 1.99) | Application Number          |    | 10580092       |  |
|--|-----------------------------|----|----------------|--|
|  | Filing Date                 |    | 2007-04-18     |  |
|  | First Named Inventor Erriko |    | cos Pitsos     |  |
|  | Art Unit                    |    | 2131           |  |
|  | Examiner Name               |    |                |  |
|  | Attorney Docket Number      | er | 310141.401USPC |  |

|                          |            |                               |                           |                     | U.S.                              | PATENTS              |   |         |  |  |
|--------------------------|------------|-------------------------------|---------------------------|---------------------|-----------------------------------|----------------------|---|---------|--|--|
| Examiner<br>Initial*     | Cite<br>No | Patent Number                 | Kind<br>Code <sup>1</sup> | issue D             | ate                               | of cited Document    |   |         | s,Columns,Lines where<br>vant Passages or Releve<br>es Appear                |  |
|                          | 1          | 4309569                       |                           | 1982-01             | -05                               | Merkle               |   |         |  |  |
|                          | 2          | 4881264                       |                           | 1989-11             | -14                               | Merkle               |   |         |  |  |
|                          | 3          | 5903651                       |                           | 1999-05             | j <b>-</b> 11                     | Kocher               |   |         |  |  |
|                          | 4          | 6065008                       |                           | 2000-05             | i-16                              | Simon et al.         |   |         |  |  |
| If you wis               | h to a     | dd additional U.S. Pater      | nt citatio                | n inform            | ation pl                          | ease click the       | Add button.                                     |         |  |  |
|                          |            |                               | U.S.P                     | ATENT               | APPLI                             | CATION PUBI          | LICATIONS                                       |         |  |  |
| Examiner<br>Initial*     | Cite<br>No | Publication Number            | Kind<br>Code <sup>1</sup> | Publica<br>Date     |                                   |                      | Name of Patentee or Applicant of cited Document |         | Pages,Columns,Lines where<br>Relevant Passages or Relevant<br>Figures Appear |  |
|                          | 1          |                               |                           |                     |                                   |                      |   |         |  |  |
| If you wis               | h to a     | l<br>dd additional U.S. Publi | shed Ap                   | plication           | citatio                           | ı<br>n information p | lease click the Add                             | d butto | n.   |  |
| FOREIGN PATENT DOCUMENTS |            |                               |                           |                     |                                   |                      |   |         |  |  |
| Examiner<br>Initial*     | Cite<br>No |                               |                           | Publication<br>Date | Applicant of cited where Relevant |                      | Passages or Relevant                            | T5      |  |  |

## INFORMATION DISCLOSURE STATEMENT BY APPLICANT

( Not for submission under 37 CFR 1.99)

| Application Number          |  | 10580092       |  |  |
|-----------------------------|--|----------------|--|--|
| Filing Date                 |  | 2007-04-18     |  |  |
| First Named Inventor Erriko |  | os Pitsos      |  |  |
| Art Unit                    |  | 2131           |  |  |
| Examiner Name               |  |                |  |  |
| Attorney Docket Number      |  | 310141.401USPC |  |  |

| 1  | 0932109   | EP   | A2   | 1999-07-28  | Yeda Research &<br>Development Company,<br>Ltd.   |  |  |  |
|--|---|--|--|---|---|--|--|--|
| 2  | 1164746   | EP   | A2   | 2001-12-19  | Silvio Micali   |  |  |  |
| h to ac  | dd additional Foreign Pa  | atent Document   | citation   | information p   | lease click the Add butto   | n  | 1  |  |
|  |   | NON-PATE   | NT LITE  | ERATURE DO  | CUMENTS   |  |  |  |
| Examiner Initials*  Cite No  Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published. |   |  |  |   |   |  |  |  |
| 1  | Brandner et al., "Archive Time-Stamps Syntax (ATS)," Internet-Draft, July 2003, URL=http://ftp.scarlet.be/pub/documentation/internet-drafts/draft-bradner-etal-ats-00.txt, 18 pages.  |  |  |   |   |  |  |  |
| 2  | Capkun et al., "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," Ecole Polytechnique Federale De Lausanne Technical Report, May 28, 2002, URL=http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf, 17 pages. |  |  |   |   |  |  |  |
| 3  | Caronni, "Walking the Web of Trust," IEEE No. 0-7695-0798-9/00, 2000, 6 pages.  |  |  |   |   |  |  |  |
| 4  | Chapweske et al., "Tree Hash EXchange Format (THEX)," Online Document, March 4, 2003, URL=http://www.open-content.net/specs/draft-jchapweske-thex-02-html, 7 pages.   |  |  |   |   |  |  |  |
| 5  | Devanbu et al., "Flexible authentication of XML documents," Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, November 5, 2001, 10 pages.  |  |  |   |   |  |  |  |
| 6  | Elwailly et al., "QuasiModo: More Efficient Hash Tree-Based Certificate Revocation," Online, September 5, 2003, URL=http://www.docomolabs-usa.com/researchers/ZRamzan/quasi-modo-v1.pdf, 7 pages.   |  |  |   |   |  |  |  |
| 7  | Feisthammel, "Explanation of the web of trust of PGP," Online, June 19, 2002, URL=http://www.rubin.ch/pgp/weboftrust.en.html, 3 pages.  |  |  |   |   |  |  |  |
|  | 2 Cite No 1 2 3 4 5 6   | 2 1164746  Cite No Include name of the authook, magazine, journ publisher, city and/or of publis | 2 1164746 EP  In to add additional Foreign Patent Document  NON-PATEI  Cite No Include name of the author (in CAPIT/ (book, magazine, journal, serial, symp publisher, city and/or country where proposed documentation/internet-drafts/draft-bradnes  Capkun et al., "Archive Time-Stamps Syndocumentation/internet-drafts/draft-bradnes  Capkun et al., "Self-Organized Public-Key De Lausanne Technical Report, May 28, 2 IC_TECH_REPORT_200234.pdf, 17 pages  Caronni, "Walking the Web of Trust," IEEE  Chapweske et al., "Tree Hash EXchange I content.net/specs/draft-jchapweske-thex-Content.net/specs/draft-jchapwesk | 2 1164746 EP A2  In to add additional Foreign Patent Document citation  NON-PATENT LITE  Cite No Include name of the author (in CAPITAL LET (book, magazine, journal, serial, symposium, publisher, city and/or country where publisher  Brandner et al., "Archive Time-Stamps Syntax (AT documentation/internet-drafts/draft-bradner-etal-at documentation/internet-drafts/draft-bradner-etal-at IC_TECH_REPORT_200234.pdf, 17 pages.  Capkun et al., "Self-Organized Public-Key Manage De Lausanne Technical Report, May 28, 2002, UF IC_TECH_REPORT_200234.pdf, 17 pages.  Caronni, "Walking the Web of Trust," IEEE No. 0-7  Chapweske et al., "Tree Hash EXchange Format (content.net/specs/draft-jchapweske-thex-02-html,  Devanbu et al., "Flexible authentication of XML do and Communications Security, Philadelphia, Penn  Elwailly et al., "QuasiModo: More Efficient Hash T URL=http://www.docomolabs-usa.com/researchers | 2 1164746 EP A2 2001-12-19  n to add additional Foreign Patent Document citation information p  NON-PATENT LITERATURE DO  Cite (book, magazine, journal, serial, symposium, catalog, etc), publisher, city and/or country where published.  Brandner et al., "Archive Time-Stamps Syntax (ATS)," Internet-Dr. documentation/internet-drafts/draft-bradner-etal-ats-00.txt, 18 pag  Capkun et al., "Self-Organized Public-Key Management for Mobile De Lausanne Technical Report, May 28, 2002, URL=http://icwww.IC_TECH_REPORT_200234.pdf, 17 pages.  Caronni, "Walking the Web of Trust," IEEE No. 0-7695-0798-9/00,  Chapweske et al., "Tree Hash EXchange Format (THEX)," Online content.net/specs/draft-jchapweske-thex-02-html, 7 pages.  Devanbu et al., "Flexible authentication of XML documents," Proceased Communications Security, Philadelphia, Pennsylvania, Noven and Communications Security, Philadelphia, Pennsylvania, Noven Elwailly et al., "QuasiModo: More Efficient Hash Tree-Based Cert URL=http://www.docomolabs-usa.com/researchers/ZRamzan/qua | 1 0932109 EP A2 1999-07-28 Development Company, Ltd.  1 164746 EP A2 2001-12-19 Silvio Micali  1 to add additional Foreign Patent Document citation information please click the Add button NON-PATENT LITERATURE DOCUMENTS  Cite No Include name of the author (in CAPITAL LETTERS), title of the article (when approping publisher, city and/or country where published.  Brandner et al., "Archive Time-Stamps Syntax (ATS)," Internet-Draft, July 2003, URL=http://ft.documentation/internet-drafts/draft-bradner-etal-ats-00.txt, 18 pages.  Capkun et al., "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," Ecole De Lausanne Technical Report, May 28, 2002, URL=http://icwww.epfl.ch/publications/documents/personality/licy/licy/licy/licy/licy/licy/licy/lic | 1 164746 EP A2 1999-07-28 Development Company, Ltd.  1 1164746 EP A2 2001-12-19 Silvio Micali  1 to add additional Foreign Patent Document citation information please click the Add button  NON-PATENT LITERATURE DOCUMENTS    Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.    Brandner et al., "Archive Time-Stamps Syntax (ATS)," Internet-Draft, July 2003, URL=http://ftp.scarlet.be/pub/documentation/internet-drafts/draft-bradner-etal-ats-00.txt, 18 pages.    Capkun et al., "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," Ecole Polytechnique Federale De Lausanner Technical Report, May 28, 2002, URL=http://icwwwi.epfl.ch/publications/documents/   UC_TECH_REPORT_200234.pdf, 17 pages.    Caronni, "Walking the Web of Trust," IEEE No. 0-7695-0798-9/00, 2000, 6 pages.    Chapweske et al., "Tree Hash Exchange Format (THEX)," Online Document, March 4, 2003, URL=http://www.opencontent.net/specs/draft-jchapweske-thex-02-html, 7 pages.    Devanbu et al., "Flexible authentication of XML documents," Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, November 5, 2001, 10 pages.    Elwailly et al., "QuasiModo: More Efficient Hash Tree-Based Certificate Revocation," Online, September 5, 2003, URL=http://www.docomolabs-usa.com/researchers/ZRamzan/quasi-modo-v1.pdf, 7 pages. |  |

## INFORMATION DISCLOSURE STATEMENT BY APPLICANT

( Not for submission under 37 CFR 1.99)

| Application Number          |  | 10580092       |  |  |
|-----------------------------|--|----------------|--|--|
| Filing Date                 |  | 2007-04-18     |  |  |
| First Named Inventor Erriko |  | s Pitsos       |  |  |
| Art Unit                    |  | 2131           |  |  |
| Examiner Name               |  |                |  |  |
| Attorney Docket Number      |  | 310141.401USPC |  |  |

|   | 8                              | Henson, "An Analysis of Compare-by-hash," Proceedings of the HOTOS-IX Full Program, Online, May 12, 2003, URL: http://www.nmt.edu/{val/review/hash.pdf, 6 pages.   |   |      |  |  |  |  |  |
|---|--------------------------------|--|---|------|--|--|--|--|--|
|   | 9                              | Aberer et al., "A decentralized public key infrastructure for customer-to-customer e-commerce," Ecole Polytechnique Federale De Lausanne Technical Report, Online, November 20, 2003, URL=http://icwww.epfl.ch/publications/ [documents/IC_TECH_REPORT_200374.pdf, 11 pages. |   |      |  |  |  |  |  |
|   | 10                             |  | Menezes et al., "Hash Functions and Data Integrity," Handbook of Applied Cryptography, CRC Press Series on Discrete Matthematics and Its Applications, Boca Raton, Florida, 1997, Chapter 9, 63 pages.  |      |  |  |  |  |  |
|   | 11                             | Zimmerman et al., "An Introduction to Cryptography," Network Associates, Inc., California, 1990-1999, 87 pages.  |   |      |  |  |  |  |  |
| If you wis  | h to a                         | dd add   | ditional non-patent literature document citation information please click the Add button  | _    |  |  |  |  |  |
|   |                                |  | EXAMINER SIGNATURE  |      |  |  |  |  |  |
| Examiner  | r Signa                        | ature  | Date Considered   |      |  |  |  |  |  |
| *EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant. |                                |  |   |      |  |  |  |  |  |
| Standard ST   | T.3). <sup>3</sup> l<br>cument | For Japa<br>t by the a   | TO Patent Documents at <a href="https://www.USPTO.GOV">www.USPTO.GOV</a> or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO panese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent docume appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here ion is attached. | ent. |  |  |  |  |  |